Granskning dataskyddsarbetet SR-2021-93

Gymnasie- och vuxenutbildningsnämnden

Nämndens yttranden till revisorskollegiet ska följa nedanstående struktur.

Första yttrande till revisorskollegiet

I det första yttrandet ska nämnden inkomma med ett sammanfattande svar utifrån granskningens slutsats som redovisas i rapporten.

Nämnden ska redovisa vilka åtgärder som planeras att genomföras, deras förväntade effekt och när de senast ska vara genomförda. Redovisningen görs separat för varje bedömning/rekommendation.

Granskningens bedömningar och rekommendationer

- Bedömningen är att dataskyddsarbetet inom Malmö stad delvis organiserats på ett tydligt och ändamålsenligt sätt och att det bedrivs ett effektivt arbete.

  Nämnderna förlitar sig i hög utsträckning på processer, rutiner och arbetssätt från kommunstyrelsen. I varierande grad har man tagit fram anpassade varianter av dessa, men resursbrist gör ofta att arbetet inte når en tillräckligt hög nivå. När varje förvaltning själva ska ta fram sina processer och rutiner blir det mindre effektivt än om en större del av arbetet gjorts centralt.

- Bedömningen är att de olika rollerna i Malmö stads dataskyddsarbete delvis är tydliga.

  Rollerna kopplade till dataskyddsarbetet har definierats och dokumenterats. Det är dock inte säkerställt att befintliga rollbeskrivningar efterlevs i praktiken. I granskningen framkommer att det råder viss osäkerhet i relation till ansvarsfördelningen samt när olika roller ska involveras och inte. Den nuvarande beskrivningen av roller inte är tillräckligt tydlig för att säkerställa ett systematiskt och standardiserat arbetssätt.

- Bedömningen är att det inte avsätts tillräckliga resurser (exempelvis personella och ekonomiska) för ett tillräckligt dataskyddsarbete.

Malmö stad

I granskningen framkommer att de intervjuade upplever att det saknas resurser för att bedriva ett önskvärt dataskyddsarbete. Exempelvis saknas resurser för att kunna säkerställa att systemägare har den kunskap och tid som behövs för att leva upp till definierad kravställning.

- Bedömningen är att det delvis bedrivs ett aktivt och strukturerat dataskyddsarbete där dataskyddsfrågor beaktas vid befintliga och tillkommande behandlingar av personuppgifter.

  I granskningen noteras att kommunstyrelsen och nämnderna bedriver ett strukturerat dataskyddsarbete vid nya behandlingar av personuppgifter och vid upphandling av nya system. Det saknas dock systematik och dokumenterade processer för att över tid granska efterlevnad av riktlinjer och rutiner för befintliga behandlingar och IT-system.

- Bedömningen är att det delvis säkerställs att dataskyddsombudet och/eller förvaltningarnas dataskyddssamordnare blir involverade vid styrelsens/nämndernas behandlingar av personuppgifter (exempelvis vid nya personuppgiftsbehandlingar vid inköp av nya IT-system).

  I de kommungemensamma riktlinjerna beskrivs att dataskyddssamordnare bör involveras inom samtliga steg i ett systems livscykel gällande klassificering. I granskningen framkommer dock att det inte säkerställts att registerförteckningar är kompletta. Således går det inte att bekräfta att DSO eller samordnare har översikt över, samt varit involverade i, samtliga behandlingar.

- Bedömningen är att personuppgiftsincidenter delvis hanteras i enlighet med lagkrav och Malmö stads riktlinjer och att Malmö stads riktlinjer för att hantera personuppgiftsincidenter delvis är tillräckliga.

  Det finns en central rutin för hantering av personuppgiftsincidenter i enlighet med lagkrav. Rutinen har dock inte anpassats utifrån respektive nämnds förutsättningar. Det har ej heller säkerställts att de dokumenterade rutinerna efterlevs i praktiken.

- Bedömningen är att det inte genomförs kontroll, uppföljning och återrapportering av Malmö stads dataskyddsarbete.

  Det finns ett flertal dokumenterade rutiner och styrdokument. Det är dock inte säkerställt att dessa efterlevs i praktiken. Mycket begränsad granskning och uppföljning sker. Vid de tillfällen någon form av uppföljning gjort så är det initierat från kommunstyrelsen. Granskningsplan eller liknande saknas helt.

Kommunstyrelsen och samtliga granskade nämnder rekommenderas att:

- Inledningsvis:
    - Utarbeta en tydlig plan för granskning och uppföljning av arbetet med dataskyddsförordningen.
    - Tillse att ansvarsfördelningen i arbetet kopplat till dataskyddsförordningen är tydligt definierad samt efterlevs i praktiken.
- Därefter:
    - Utveckla rutinen för klassificering av informationstillgångar med avseende på ostrukturerad data. Utarbeta en dokumenterad rutin för uppföljning av registerförteckningens riktighet och fullständighet över tid.
    - Utarbeta rutiner som över tid säkerställer att personuppgifter endast behandlas för det eller de ändamål som de samlades in för.
    - Utarbeta dokumenterade rutiner för att säkerställa att personuppgiftsbiträden och leverantörer uppfyller och agerar i enlighet med dataskyddsförordningen över tid.
    - Säkerställa tillräcklig kontroll över att incidenthanteringsrutinen efterlevs i praktiken.

Gymnasie-och vuxenutbildningsnämnden rekommenderas att:

- Inledningsvis:
    - Tillse att registerförteckningen är komplett samt förblir uppdaterad över tid.
    - Utarbeta en rutin som säkerställer att centralt framtagna styrdokument anpassas utefter den egna verksamheten.
    - Strukturerat genomföra riskanalyser och konsekvensbedömningar enligt dokumenterad rutin.
    - Säkerställa att det finns tillräckligt med resurser för att utföra ett ändamålsenligt arbete kopplat till dataskyddsförordningen.
- Därefter:
    - Ta fram en rutin för att säkerställa att gallring av personuppgiftsbehandlingar utförs enligt definierad process.

- Utarbeta en dokumenterad rutin för hur systemägare ska utföra behörighetskontroller i gymnasie- och vuxenutbildningsnämndens IT-system.

- Ta fram och dokumentera en rutin för att säkerställa att tillräcklig information loggas i samband med incidentrapportering.

Uppföljande yttrande till revisorskollegiet

I det uppföljande yttrandet ska nämnden inkomma med ett sammanfattande svar utifrån granskningens slutsats som redovisas i rapporten.

Nämnden ska redovisa vilka åtgärder som har vidtagits under 2022 och redogöra för vilken effekt dessa haft i verksamheten. Redovisningen görs separat för varje bedömning/rekommendation, på samma vis som det första yttrandet.